



---

## **7206 VXR NPE-400 Router with VPN Acceleration Module (VAM)**



## **FIPS 140-2 Non-Proprietary Security Policy**

**Level 2 Validation  
Version 1.1**

**April 21, 2004**

# Table of Contents

<b>INTRODUCTION.....</b>	<b>3</b>
PURPOSE .....	3
REFERENCES .....	3
DOCUMENT ORGANIZATION .....	3
<b>CISCO 7206 VXR NPE-400 WITH VAM .....</b>	<b>5</b>
OVERVIEW .....	5
CRYPTOGRAPHIC MODULE .....	5
MODULE INTERFACES .....	6
ROLES AND SERVICES.....	9
<i>Crypto Officer Services</i> .....	10
<i>User Services</i> .....	10
PHYSICAL SECURITY .....	11
CRYPTOGRAPHIC KEY MANAGEMENT .....	13
SELF-TESTS.....	18
<b>SECURE OPERATION .....</b>	<b>20</b>

## Introduction

### ***Purpose***

This is a non-proprietary Cryptographic Module Security Policy for Cisco Systems. This security policy describes how the 7206 VXR NPE-400 with VPN Acceleration Module (VAM) (Hardware Version: 7206-VXR; VAM: Hardware Version 1.0, Board Version A0; Firmware Version: IOS 12.3(3d)) meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

Note: This document may be copied in its entirety and without modification. All copies must include the copyright notice and statements on the last page.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at <http://csrc.nist.gov/cryptval/>.

### ***References***

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Cisco Systems, Inc. website ([www.cisco.com](http://www.cisco.com)) contains information on the full line of products from Cisco Systems, Inc.
- The NIST Validated Modules website (<http://csrc.ncsl.nist.gov/cryptval/>): contains contact information for answers to technical or sales-related questions for the module

### ***Document Organization***

The Security Policy document is one document in the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is proprietary to Cisco Systems, Inc. and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems, Inc.

## Cisco 7206 VXR NPE-400 WITH VAM

### *Overview*

The 7206 VXR router is designed to support gigabit capabilities and to improve data, voice, and video integration in both service provider and enterprise environments. Cisco 7206 VXR routers support a high-speed network services engine (NSE) as well as the high-speed network processing engine, NPE-400, and all other available network processing engines.

Cisco 7206 VXR routers accommodate a variety of network interface port adapters and an I/O controller. A Cisco 7206 VXR router equipped with an NPE-400 can support up to six high-speed port adapters and can also support higher-speed port adapter interfaces including Gigabit Ethernet and OC-12 ATM. Cisco 7206 VXR routers also contain bays for up to two AC-input or DC-input power supplies.

Cisco 7206 VXR routers support the following features:

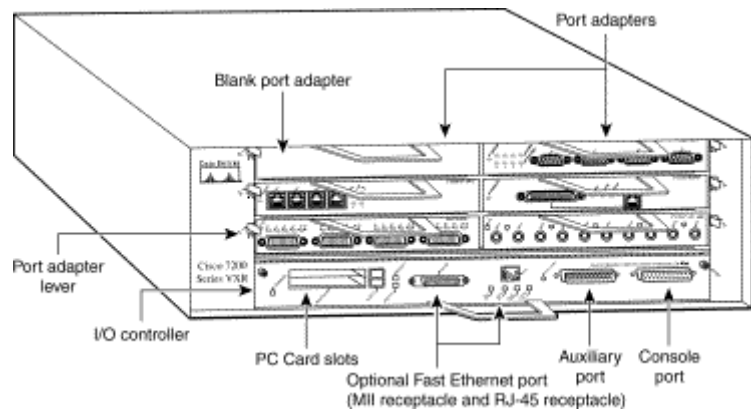
- Online insertion and removal (OIR)—Add, replace, or remove port adapters without interrupting the system.
- Dual hot-swappable, load-sharing power supplies—Provide system power redundancy; if one power supply or power source fails, the other power supply maintains system power without interruption. Also, when one power supply is powered off and removed from the router, the second power supply immediately takes over the router power requirements without interrupting normal operation of the router.
- Environmental monitoring and reporting functions—Maintain normal system operation by resolving adverse environmental conditions prior to loss of operation.
- Downloadable software—Load new images into Flash memory remotely, without having to physically access the router.

The Cisco 7206 VXR router incorporates a single VPN Acceleration Module (VAM) cryptographic accelerator card. The VAM is installed in one of the port adapter slots.

### *Cryptographic Module*

The Cisco 7206 VXR with VAM is a multiple-chip standalone cryptographic module. The Cisco 7206VXR supports multi-protocol

routing and bridging with a wide variety of protocols and port adapter combinations available for Cisco 7200 series routers. The metal casing that fully encloses the module establishes the cryptographic boundary for the router, all the functionality discussed in this document is provided by components within the casing. The Cisco 7206VXR has six slots for port adapters, one slot for an input/output (I/O) controller, and one slot for a network processing engine or network services engine.



**Figure 1 - The 7206 VXR NPE-400 Router**

The NPE-400 uses an RM7000 microprocessor that operates at an internal clock speed of 350 MHz. The NPE-400 uses SDRAM for storing all packets received or sent from network interfaces. The SDRAM memory array in the system allows concurrent access by port adapters and the processor. The NPE-400 has three levels of cache: a primary and a secondary cache that are internal to the microprocessor, and a tertiary 4-MB external cache that provides additional high-speed storage for data and instructions.

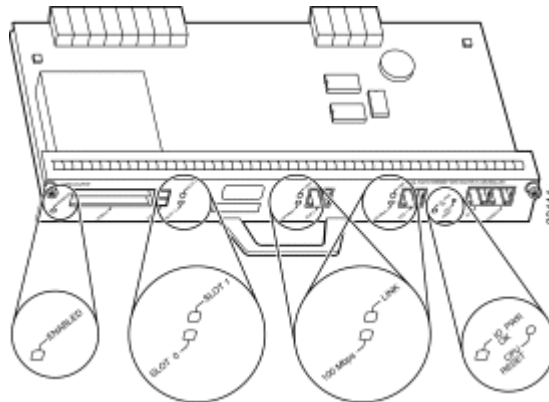
The Cisco 7206VXR router comes equipped with one 280W AC-input power supply. (A 280W DC-input power supply option is available.) A power supply filler plate is installed over the second power supply bay. A fully configured Cisco 7206VXR router operates with only one installed power supply; however, a second, optional power supply of the same type provides hot-swappable, load-sharing, redundant power.

## ***Module Interfaces***

The interfaces for the router are located on the front panel Input/Output (I/O) Controller, with the exception of the power switch and power plug. The module has two Fast Ethernet (10/100 RJ-45) connectors for data transfers in and out. The module also has two other RJ-45 connectors for

a console terminal for local system access and an auxiliary port for remote system access or dial backup using a modem.

The figure below shows the front panel LEDs, which provide overall status of the router operation. The front panel displays whether or not the router is booted, if the redundant power is attached and operational, and overall activity/link status.



**Figure 2 – Front Panel LEDs**

LED	Indication	Description
Enabled	Green	Indicates that the network processing engine or network services engine and the I/O controller are enabled for operation by the system; however, it does not mean that the Fast Ethernet port on the I/O controller is functional or enabled. This LED goes on during a successful router boot and remains on during normal operation of the router.
IO POWER OK	Amber	Indicates that the I/O controller is on and receiving DC power from the router midplane. This LED comes on during a successful router boot and remains on during normal operation of the router.
	Off	Powered off or failed.
Slot 0 Slot 1	Green	These LEDs indicate which PC Card slot is in use by coming on when either slot is being accessed by the system. These LEDs remain off during normal operation of the router.
Link	Green	Indicates that the Ethernet RJ-45 receptacle has established a valid link with the network.
	Off	This LED remains off during normal operation of the router unless there is an incoming carrier signal.
100 Mbps	Green	Indicates that the port is configured for 100-Mbps operation (speed 100), or if configured for auto negotiation (speed auto), the port has detected a valid link at 100 Mbps.
	Off	If the port is configured for 10-Mbps operation, or if it is configured for auto negotiation and the port has detected a valid link at 10 Mbps, the LED remains off.

**Table 1 – Front Panel LEDs and Descriptions**

The VPN Acceleration Module (VAM) is a single-width acceleration module that provides high-performance, hardware-assisted tunneling and encryption services suitable for virtual private network (VPN) remote access, site-to-site intranet, and extranet applications. It also provides platform scalability and security while working with all services necessary for successful VPN deployments—security, quality of service (QoS), firewall and intrusion detection, and service-level validation and management. The VAM off-loads IPsec processing from the main processor, thus freeing resources on the processor engines for other tasks.

The VAM has three LEDs, as shown below. Table 2 lists the colors and functions of the VAM LEDs.

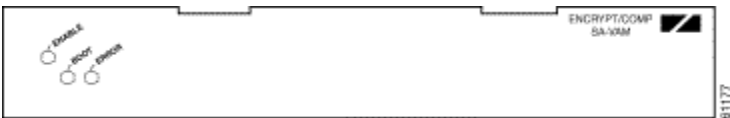


Figure 3 – VAM LEDs

LED Label	Color	State	Function
ENABLE	Green	On	Indicates the VAM is powered up and enabled for operation.
BOOT	Amber	Pulses	Indicates the VAM is operating.
		On	Indicates the VAM is booting or a packet is being encrypted or decrypted.
ERROR	Amber	On	Indicates an encryption error has occurred. This LED is normally off.

Table 2 – VAM LEDs and Descriptions

All of these physical interfaces are separated into the logical interfaces from FIPS as described in the following table:

Router Physical Interface	FIPS 140-2 Logical Interface
10/100BASE-TX LAN Port Port Adapter Interface Console Port Auxiliary Port PCMCIA Slot	Data Input Interface
10/100BASE-TX LAN Port Port Adapter Interface Console Port Auxiliary Port PCMCIA Slot	Data Output Interface
Power Switch Console Port Auxiliary Port	Control Input Interface



Router Physical Interface	FIPS 140-2 Logical Interface
10/100BASE-TX LAN Port LEDs Enabled LED PCMCIA LEDs IO Pwr Ok LED VAM LEDs Console Port Auxiliary Port	Status Output Interface
Power Plug	Power Interface

**Table 3 – FIPS 140-2 Logical Interfaces**

In addition to the built-in interfaces, the router also has additional port adapters that can optionally be placed in an available slot. These port adapters have many embodiments, including multiple Ethernet, token ring, and modem cards to handle frame relay, ATM, and ISDN connections. (Note: These additional port adapters were excluded from this FIPS 140-2 Validation.)

### ***Roles and Services***

Authentication is role-based. There are two main roles in the router that operators may assume: the Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services. Both roles are authenticated by providing a valid username and password. The configuration of the encryption and decryption functionality is performed only by the Crypto Officer after authentication to the Crypto Officer role by providing a valid Crypto Officer username and password. Once the Crypto Officer configured the encryption and decryption functionality, the User can use this functionality after authentication to the User role by providing a valid User username and password. The Crypto Officer can also use the encryption and decryption functionality after authentication to the Crypto Officer role. The module supports RADIUS and TACACS+ for authentication and they are used in the FIPS mode. A complete description of all the management and configuration capabilities of the Cisco 7206 Router can be found in the *Performing Basic System Management* manual and in the online help for the router.

The User and Crypto Officer passwords and the RADIUS/TACACS+ shared secrets must each be at least 8 alphanumeric characters in length. See the *Secure Operation* section for more information. If only integers 0-9 are used without repetition for an 8 digit PIN, the probability of randomly guessing the correct sequence is 1 in 1,814,400. Including the rest of the alphanumeric characters drastically decreases the odds of guessing the correct sequence.

### *Crypto Officer Services*

During initial configuration of the router, the Crypto Officer password (the “enable” password) is defined. A Crypto Officer may assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration and maintenance of the router. The Crypto Officer services consist of the following:

- **Configure the router:** define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.
- **Define Rules and Filters:** create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- **Status Functions:** view the router configuration, routing tables, active sessions, use Gets to view SNMP MIB II statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status
- **Manage the router:** log off users, shutdown or reload the router, manually back up router configurations, view complete configurations, manager user rights, and restore router configurations.
- **Set Encryption/Bypass:** set up the configuration tables for IP tunneling. Set keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.
- **Change Port Adapters:** insert and remove Port Adapters in the Port Adapter slots.

### *User Services*

A User enters the system by accessing the console port with a terminal program. The IOS prompts the User for their password. If the password is correct, the User is allowed entry to the IOS executive program. The services available to the User role consist of the following:

- **Status Functions:** view state of interfaces, state of layer 2 protocols, version of IOS currently running

- **Network Functions:** connect to other network devices through outgoing telnet, PPP, etc. and initiate diagnostic network services (i.e., ping, mtrace)
- **Terminal Functions:** adjust the terminal session (e.g., lock the terminal, adjust flow control)
- **Directory Services:** display directory of files kept in flash memory

### ***Physical Security***

The router is entirely encased by a thick steel chassis. The front of the router provides 6 port adapter slots, on-board LAN connectors, PC Card slots, and Console/Auxiliary connectors. The power cable connection, a power switch, and the access to the Network Processing Engine are at the rear of the router.

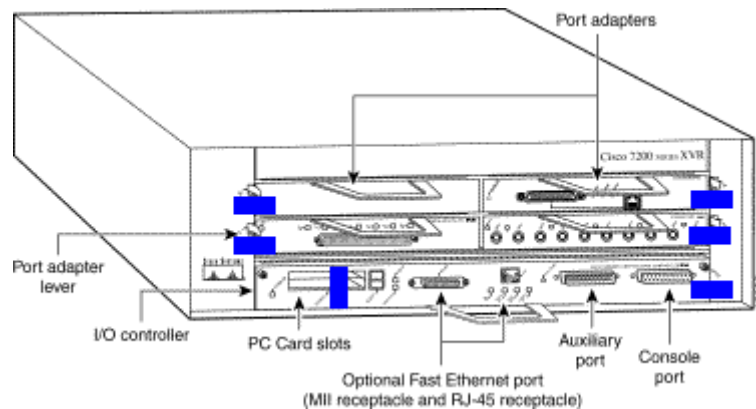
Any Port Adapter slot, which is not populated with a Port Adapter, must be populated with an appropriate slot cover in order to operate in a FIPS compliant mode. The slot covers are included with each router, and additional covers may be ordered from Cisco. The same procedure mentioned below to apply tamper evidence labels for Port Adapters must also be followed to apply tamper evidence labels for the slot covers.

Once the router has been configured to meet FIPS 140-2 Level 2 requirements, the router cannot be accessed without signs of tampering. To seal the system, apply serialized tamper-evidence labels as follows:

- Clean the cover of any grease, dirt, or oil before applying the tamper evidence labels. Alcohol-based cleaning pads are recommended for this purpose. The ambient air must be above 10C, otherwise the labels may not properly cure.
- The tamper evidence label should be placed so that the one half of the label covers the enclosure and the other half covers the 7206 VXR NPE-400 Input/Output Controller.
- The tamper evidence label should be placed over the Flash PC Card slots on the Input/Output Controller.
- The tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the port adapter slot 1.
- The tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the port adapter slot 2.

- The tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the port adapter slot 3.
- The tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the port adapter slot 4.
- The tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the port adapter slot 5.
- The tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the port adapter slot 6.
- The tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the network processing engine.
- The tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the power supply plate.
- The tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the redundant power supply plate.

The labels completely cure within five minutes.



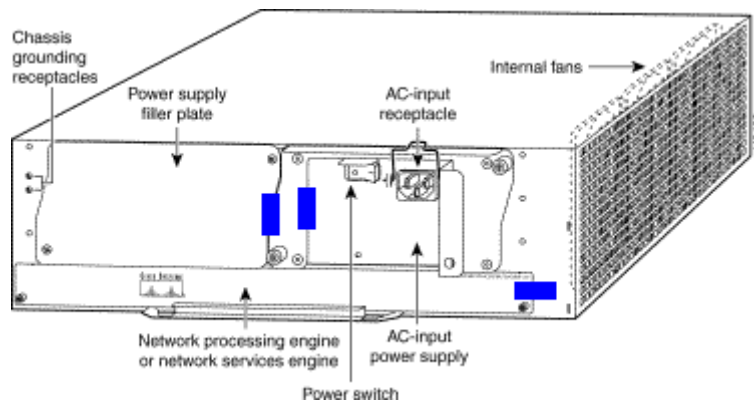


Figure 4 – Tamper Evidence Label Placement

## Cryptographic Key Management

The router securely administers both cryptographic keys and other critical security parameters such as passwords. The tamper evidence seals provide physical protection for all keys. All keys are also protected by the password-protection on the Crypto Officer role login, and can be zeroized by the Crypto Officer. Keys are exchanged manually and entered electronically via manual key exchange or Internet Key Exchange (IKE).

The modules contain a cryptographic accelerator card (the VAM), which provides DES (56-bit) (only for legacy systems), and 3DES (168-bit) IPsec encryption, MD5 and SHA-1 hashing, and has hardware support for DH and RSA key generation.

The module supports the following critical security parameters (CSPs):

#	CSP Name	Description	Storage
1	CSP 1	This is the seed key for X9.31 PRNG. This key is stored in DRAM and updated periodically after the generation of 400 bytes; hence, it is zeroized periodically. Also, the operator can turn off the router to zeroize this key.	DRAM (plaintext)
2	CSP 2	The private exponent used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated.	DRAM (plaintext)
3	CSP 3	The shared secret within IKE exchange. Zeroized when IKE session is terminated.	DRAM (plaintext)
4	CSP 4	Same as above	DRAM (plaintext)
5	CSP 5	Same as above	DRAM

			(plaintext)
6	CSP 6	Same as above	DRAM (plaintext)
7	CSP 7	The IKE session encrypt key. The zeroization is the same as above.	DRAM (plaintext)
8	CSP 8	The IKE session authentication key. The zeroization is the same as above.	DRAM (plaintext)
9	CSP 9	The RSA private key. "crypto key zeroize" command zeroizes this key.	NVRAM (plaintext)
10	CSP 10	The key used to generate IKE skedid during preshared-key authentication. "no crypto isakmp key" command zeroizes it. This key can have two forms based on whether the key is related to the hostname or the IP address.	NVRAM (plaintext)
11	CSP 11	This key generates keys 3, 4, 5 and 6. This key is zeroized after generating those keys.	DRAM (plaintext)
12	CSP 12	The RSA public key used to validate signatures within IKE. These keys are expired either when CRL (certificate revocation list) expires or 5 secs after if no CRL exists. After above expiration happens and before a new public key structure is created this key is deleted. This key does not need to be zeroized because it is a public key; however, it is zeroized as mentioned here.	DRAM (plaintext)
13	CSP 13	The fixed key used in Cisco vendor ID generation. This key is embedded in the module binary image and can be deleted by erasing the Flash.	NVRAM (plaintext)
14	CSP 14	The IPSec encryption key. Zeroized when IPSec session is terminated.	DRAM (plaintext)
15	CSP 15	The IPSec authentication key. The zeroization is the same as above.	DRAM (plaintext)
16	CSP 16	The RSA public key of the CA. "no crypto ca trust <label>" command invalidates the key and it frees the public key label which in essence prevent use of the key. This key does not need to be zeroized because it is a public key.	NVRAM (plaintext)
17	CSP 17	This key is a public key of the DNS server. Zeroized using the same mechanism as above. "no crypto ca trust <label>" command invalidate the DNS server's public key and it frees the public key label which in essence prevent use of that key. This label is different from the label in the above key. This key does not need to be zeroized because it is a public key.	NVRAM (plaintext)
18	CSP 18	The SSL session key. Zeroized when the SSL connection is terminated.	DRAM (plaintext)

19	CSP 19	The ARAP key that is hardcoded in the module binary image. This key can be deleted by erasing the Flash.	Flash (plaintext)
20	CSP 20	This is an ARAP user password used as an authentication key. A function uses this key in a DES algorithm for authentication.	DRAM (plaintext)
21	CSP 21	The key used to encrypt values of the configuration file. This key is zeroized when the “no key config-key” is issued.	NVRAM (plaintext)
22	CSP 22	This key is used by the router to authenticate itself to the peer. The router itself gets the password (that is used as this key) from the AAA server and sends it onto the peer. The password retrieved from the AAA server is zeroized upon completion of the authentication attempt.	DRAM (plaintext)
23	CSP 23	The RSA public key used in SSH. Zeroized after the termination of the SSH session. This key does not need to be zeroized because it is a public key; However, it is zeroized as mentioned here.	DRAM (plaintext)
24	CSP 24	The authentication key used in PPP. This key is in the DRAM and not zeroized at runtime. One can turn off the router to zeroize this key because it is stored in DRAM.	DRAM (plaintext)
25	CSP 25	This key is used by the router to authenticate itself to the peer. The key is identical to #22 except that it is retrieved from the local database (on the router itself). Issuing the “no username password” zeroizes the password (that is used as this key) from the local database.	NVRAM (plaintext)
26	CSP 26	This is the SSH session key. It is zeroized when the SSH session is terminated.	DRAM (plaintext)
27	CSP 27	The password of the User role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
28	CSP 28	The plaintext password of the CO role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
29	CSP 29	The ciphertext password of the CO role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
30	CSP 30	The RADIUS shared secret. This shared secret is zeroized by executing the “no” form of the RADIUS shared secret set command.	NVRAM (plaintext), DRAM



			(plaintext)
31	CSP 31	The TACACS+ shared secret. This shared secret is zeroized by executing the “no” form of the TACACS+ shared secret set command.	NVRAM (plaintext), DRAM (plaintext)

**Table 4 – Critical Security Parameters**

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed in the Table 5.



SRDI/Role/Service Access Policy	Security Relevant Data Item	CSP 1	CSP 2	CSP 3	CSP 4	CSP 5	CSP 6	CSP 7	CSP 8	CSP 9	CSP 10	CSP 11	CSP 12	CSP 13	CSP 14	CSP 15	CSP 16	CSP 17	CSP 18	CSP 19	CSP 20	CSP 21	CSP 22	CSP 23	CSP 24	CSP 25	CSP 26	CSP 27	CSP 28	CSP 29	CSP 30	CSP 31
	Role/Service																															
	User role																															
	Status Functions																															
	Network Functions	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r											
	Terminal Functions																															
	Directory Services																															
	Crypto-Officer Role																															
	Configure the Router													r w d							r w d											
	Define Rules and Filters																															
Status Functions																																
Manage the Router	d																				r w d											
																					r w d											
Set Encryption/Bypass		r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d		r w d	r w d	r w d	r w d	r w d	r w d		r w d										
Change Port Adapters																																

Table 5 – Role and Service Access to CSPs

The module supports DES (only for legacy systems), 3DES, DES-MAC, TDES-MAC, AES, SHA-1, HMAC SHA-1, MD5, MD4, HMAC MD5, Diffie-Hellman, RSA (for digital signatures and encryption/decryption (for IKE authentication)) cryptographic algorithms. The MD5, HMAC MD5, and MD4 algorithms are disabled when operating in FIPS mode.

The module supports three types of key management schemes:

1. Manual key exchange method that is symmetric. DES/3DES/AES key and HMAC-SHA-1 key are exchanged manually and entered electronically.
2. Internet Key Exchange method with support for exchanging pre-shared keys manually and entering electronically.
  - The pre-shared keys are used with Diffie-Hellman key agreement technique to derive DES, 3DES or AES keys.
  - The pre-shared key is also used to derive HMAC-SHA-1 key.
3. Internet Key Exchange with RSA-signature authentication.

All pre-shared keys are associated with the CO role that created the keys, and the CO role is protected by a password. Therefore, the CO password is associated with all the pre-shared keys. The Crypto Officer needs to be authenticated to store keys. All Diffie-Hellman (DH) keys agreed upon for individual tunnels are directly associated with that specific tunnel only via the IKE protocol.

#### Key Zeroization:

All of the keys and CSPs of the module can be zeroized. Please refer to the Description column of Table 4 for information on methods to zeroize each key and CSP.

### **Self-Tests**

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router includes an array of self-tests that are run during startup and periodically during operations. If any of the self-tests fail, the router transitions into an error state. Within the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

Self-tests performed by the IOS image:

#### Power-up tests

- Firmware integrity test
- RSA signature KAT (both signature and verification)
- DES KAT
- TDES KAT
- AES KAT
- SHA-1 KAT
- PRNG KAT
- Power-up bypass test
- Diffie-Hellman self-test
- HMAC SHA-1 KAT

#### Conditional tests

- Conditional bypass test
- Pairwise consistency test on RSA signature
- Continuous random number generator tests

Self-tests performed by the VAM (cryptographic accelerator):

#### Power-up tests

- Firmware integrity test
- RSA signature KAT (both signature and verification)
- DES KAT
- TDES KAT
- SHA-1 KAT
- HMAC SHA-1 KAT
- PRNG KAT

#### Conditional tests

- Pairwise consistency test on RSA signature
- Continuous random number generator tests

## SECURE OPERATION

Cisco 7206 VXR NPE-400 Router with VAM meets all the Level 2 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS mode. Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation.

### Initial Setup

1. The Crypto Officer must ensure that the VAM cryptographic accelerator card is installed in the module by visually confirming the presence of the VAM in a port adapter slot.
2. The Crypto Officer must apply tamper evidence labels as described in the Physical Security section of this document.
3. Only a Crypto Officer may add and remove Port Adapters. When removing the tamper evidence label, the Crypto Officer should remove the entire label from the router and clean the cover of any grease, dirt, or oil with an alcohol-based cleaning pad. The Crypto Officer must re-apply tamper evidence labels on the router as described in the Physical Security section of this document.
4. The Crypto Officer must disable IOS Password Recovery by executing the following commands:

```
configure terminal  
  
no service password-recovery  
  
end  
  
show version
```

NOTE: Once Password Recovery is disabled, administrative access to the module without the password will not be possible.

### System Initialization and Configuration

1. The Crypto Officer must perform the initial configuration. The IOS version 12.3(3d), is the only allowable image. No other image may be loaded.
2. The value of the boot field must be 0x0101 (the factory default). This setting disables break from the console to the ROM monitor and automatically boots the IOS image. From the “configure terminal” command line, the Crypto Officer enters the following syntax:

```
config-register 0x0101
```

3. The Crypto Officer must create the “enable” password for the Crypto Officer role. The password must be at least 8 characters and is entered when the Crypto Officer first engages the “enable” command. The Crypto Officer enters the following syntax at the “#” prompt:

```
enable secret [PASSWORD]
```

4. The Crypto Officer must always assign passwords (of at least 8 characters) to users. Identification and authentication on the console port is required for Users. From the “configure terminal” command line, the Crypto Officer enters the following syntax:

```
line con 0
```

```
password [PASSWORD]
```

```
login local
```

5. The Crypto Officer shall only assign users to a privilege level 1 (the default).
6. The Crypto Officer shall not assign a command to any privilege level other than its default.
7. The Crypto Officer may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. If the module is configured to use RADIUS or TACACS+, the Crypto-Officer must define RADIUS or TACACS+ shared secret keys that are at least 8 characters long.
8. If the Crypto Officer loads any IOS image onto the router, this will put the router into a non-FIPS mode of operation.

### **IPSec Requirements and Cryptographic Algorithms**

There are two types of key management method that are allowed in FIPS mode: Internet Key Exchange (IKE) and IPSec manually entered keys.

Although the IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:

- ah-sha-hmac
- esp-des

- esp-sha-hmac
- esp-3des
- esp-aes

The following algorithms are not FIPS approved and should be disabled:

- MD-4 and MD-5 for signing
- MD-5 HMAC

#### **Protocols**

1. SNMP v3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP *gets* and *sets*. Since SNMP v2C uses community strings for authentication, only *gets* are allowed under SNMP v2C.

#### **Remote Access**

1. Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections via telnet are secured through IPSec.
2. SSH access to the module is only allowed if SSH is configured to use a FIPS-approved algorithm. The Crypto officer must configure the module so that SSH uses only FIPS-approved algorithms.

CISCO EDITOR'S NOTE: You may now include all standard Cisco documentation information (see other security policies). Be sure that the following line is in the legal statements at the end of the document:

By printing or making a copy of this document, the user agrees to use this information for product evaluation purposes only. Sale of this information in whole or in part is not authorized by Cisco Systems.